UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/645,388	08/21/2003	Edward James Norris	03-8005	8100

25537 7590 07/28/2008

VERIZON
PATENT MANAGEMENT GROUP
1515 N. COURTHOUSE ROAD
SUITE 500
ARLINGTON, VA 22201-2909

EXAMINER	
PATEL, CHANDRAHAS B	
ART UNIT	**PAPER NUMBER**
2616	

NOTIFICATION DATE	DELIVERY MODE
07/28/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@verizon.com

Office Action Summary	Application No.	Applicant(s)	
	10/645,388	NORRIS, EDWARD JAMES	
	Examiner	Art Unit	
	Chandrahas Patel	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/4/2008 has been entered.

Response to Arguments

2. Applicant's arguments with respect to claims 1, 2, 18, 19, 34, 49-52 have been considered but are moot in view of the new ground(s) of rejection. Applicant argues that the amended features are not taught by any of the references. Examiner agrees with this. However, upon further consideration Gray et al. (USPN 7,295,524) teaches the amended features of claims 1, 2, 18, 19, 34, 49-52.

Specification

3. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. **The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided.** The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

4. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Rejections - 35 USC § 103

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 1-5, 7, 10-14, 17-22, 24, 27-31, 34-37, 39, 42-46, 49-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ocepek et al. (USPN 7,124,197) in view of Gray et al. (USPN 7,295,524).

Regarding claim 1, Ocepek teaches a method for detecting a device on a network **[Col. 5, lines 14-15]**, said method comprising: receiving from the network a packet with an address **[Fig. 6, Source field is an address field which is received by security device as stated in Col. 7, lines 39-40]**; and indicating that the received packet corresponds to the device based on the address and on an operating system associated with the received packet **[Col. 7, lines 43-47, source MAC address specifies the operating system]**.

However, Ocepek in Col. 7, lines 43-47 does not teach that the device is a wireless access device as cited in the original action rather teaches that the device is a server and does not teach determining a wireless device based on the first three octets of the address.

Ocepek teaches the device can be wireless access device **[Fig. 1, 20, since WAP has a MAC address the same concept can be used to identify a wireless device]** and Gray teaches determining a wireless device based on the first three octets of the address **[Col. 14, lines 12-25]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have a check for the wireless access device so that intruder can be prevented from gaining access to internal server and servers can be protected **[Col. 2, lines 16-20]** and to match the first three octets to determine if the device is a wireless device since first three octets can identify WLAN manufacturer of the device which enables to determine if the device is a WLAN device **[Col. 14, lines 12-15]**.

Regarding claim 2, Ocepek teaches a method for detecting a device on a network **[Col. 5, lines 14-15]**, said method comprising: receiving from the network a packet with an address **[Fig. 6, Source field is an address field which is received by security device as stated in Col. 7, lines 39-40]**; comparing the address with one or more registered addresses **[Col. 8, lines 54-59]**; determining an operating system associated with the address, when said comparing the address results in a match between the address and at least one of the registered addresses **[Col. 8, lines 59-63, source MAC address can be used to determine operating system Col. 7, lines 43-44]**; comparing the determined operating system with one or more stored operating systems, such that at least one of the stored operating systems corresponds to the device **[Col. 8, lines 63-65, MAC address is used to determine and compare operating system as discussed in Col. 7, lines 43-44, each MAC address can tell the operating system since specific manufactures are assigned particular series of MAC addresses as applicant discussed in his application]**; and indicating that the received packet corresponds to the device when the determined operating system matches at least one of the stored operating systems **[Col. 7, lines 43-55]**.

However, Ocepek in Col. 7, lines 43-55 does not teach that the device is a wireless access device rather teaches the device is a server and does not teach determining a wireless device based on the first three octets of the address.

Ocepek teaches the device can be wireless access device **[Fig. 1, 20, since WAP has a MAC address the same concept can be used to identify a wireless device]** and Gray teaches determining a wireless device based on the first three octets of the address **[Col. 14, lines 12-25]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have a check for the wireless access device so that intruder can be prevented from gaining access to internal server and servers can be protected **[Col. 2, lines 16-20]** and to match the first three octets to determine if the device is a wireless device since first three octets can identify WLAN manufacturer of the device which enables to determine if the device is a WLAN device **[Col. 14, lines 12-15]**.

Regarding claims 3, 20, 35, Ocepek teaches receiving the address with information identifying a source of a packet **[Col. 8, lines 57-59]**.

Regarding claims 4, 21, 36, Ocepek teaches using an organizationally unique identifier as the information identifying the source **[Col. 8, lines 57-59, MAC address' first portion has organizationally unique identifier]**.

Regarding claims 5, 22, 37, Ocepek teaches receiving the address based on passively monitoring the network **[Col. 5, lines 22-26]**.

Regarding claims 7, 24, 39, Ocepek teaches determining whether a first organizationally unique identifier of the address is similar to a second organizationally unique identifier of at least

one of the registered addresses **[Col. 8, lines 63-65, MAC address has an organizational unique identifier in its first portion]**.

Regarding claims 10, 27, 42, Ocepek teaches indicating the wireless access device is not authorized on the network **[Col. 8, lines 59-63, a Null value of MAC address indicates the wireless device is not authorized yet]**.

Regarding claims 11, 28, 43, Ocepek teaches storing the one or more registered addresses, such that the one or more registered addresses are searchable **[Fig. 11, Col. 10, lines 49-51]**.

Regarding claims 12, 29, 44, Ocepek teaches storing a portion of at least one of the registered addresses **[Fig. 11]**.

Regarding claims 13, 30, 45, Ocepek teaches using an organizationally unique identifier as the portion **[Fig. 11, IP address and MAC address has an organizational unique identifier in its first portion]**.

Regarding claims 14, 31, 46, Ocepek teaches storing a plurality of the organizationally unique identifiers, such that the organizationally unique identifiers are searchable **[Fig. 11, Col. 10, lines 49-51]**.

Regarding claim 17, Ocepek teaches indicating that the received packet corresponds to the wireless access device when the determined operating system does not match the stored operating systems **[Col. 8, lines 63-65, it identifies the device whether operating systems matches or not]**.

Regarding claim 18, Ocepek teaches a system for detecting a device on a network **[Abstract]**, said system comprising: means for receiving from the network a packet with an

address **[Fig. 6, Source field is an address field which is received by security device as stated in Col. 7, lines 39-40]**; means for comparing the address with one or more registered addresses **[Col. 8, lines 54-59]**; means for determining an operating system associated with the address, when said comparing the address results in a match between the address and at least one of the registered addresses **[Col. 8, lines 59-63, source MAC address can be used to determine operating system Col. 7, lines 43-44]**; means for comparing the determined operating system with one or more stored operating systems, such that at least one of the stored operating systems corresponds to the device **[Col. 8, lines 63-65, MAC address is used to determine and compare operating system as discussed in Col. 7, lines 43-44, each MAC address can tell the operating system since specific manufactures are assigned particular series of MAC addresses as applicant discussed in his application]**; and means for indicating that the received packet corresponds to the device when the determined operating system matches at least one of the stored operating systems **[Col. 7, lines 43-55]**.

However, Ocepek in Col. 7, lines 43-55 does not teach that the device is a wireless access device rather teaches the device is a server and does not teach determining a wireless device based on the first three octets of the address.

Ocepek teaches the device can be wireless access device **[Fig. 1, 20, since WAP has a MAC address the same concept can be used to identify a wireless device]** and Gray teaches determining a wireless device based on the first three octets of the address **[Col. 14, lines 12-25]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have a check for the wireless access device so that intruder can be prevented from gaining access to internal server and servers can be protected **[Col. 2, lines 16-20]** and to match

the first three octets to determine if the device is a wireless device since first three octets can identify WLAN manufacturer of the device which enables to determine if the device is a WLAN device **[Col. 14, lines 12-15]**.

Regarding claim 19, Ocepek teaches a system for detecting a device on a network **[Abstract]**, said system comprising: at least one memory **[Fig. 7, 102, Col. 7, lines 60-62]** comprising: code that receives from the network a packet with an address **[Fig. 6, Source field is an address field which is received by security device as stated in Col. 7, lines 39-40]**; code that compares the address with one or more registered addresses **[Col. 8, lines 54-59]**; code that determines an operating system associated with the address, when said comparing the address results in a match between the address and at least one of the registered addresses **[Col. 8, lines 59-63, source MAC address can be used to determine operating system Col. 7, lines 43-44]**; code that compares the determined operating system with one or more stored operating systems, such that at least one of the stored operating systems corresponds to the device **[Col. 8, lines 63-65, MAC address is used to determine and compare operating system as discussed in Col. 7, lines 43-44, each MAC address can tell the operating system since specific manufactures are assigned particular series of MAC addresses as applicant discussed in his application]**; and code that indicates that the received packet corresponds to the device when the determined operating system matches at least one of the stored operating systems **[Col. 7, lines 43-55]**; and at least one data processor that executes the code **[Fig. 7, 134, Col. 8, lines 9-11]**.

However, Ocepek in Col. 7, lines 43-55 does not teach that the device is a wireless access device rather teaches the device is a server and does not teach determining a wireless device based on the first three octets of the address.

Ocepek teaches the device can be wireless access device **[Fig. 1, 20, since WAP has a MAC address the same concept can be used to identify a wireless device]** and Gray teaches determining a wireless device based on the first three octets of the address **[Col. 14, lines 12-25]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have a check for the wireless access device so that intruder can be prevented from gaining access to internal server and servers can be protected **[Col. 2, lines 16-20]** and to match the first three octets to determine if the device is a wireless device since first three octets can identify WLAN manufacturer of the device which enables to determine if the device is a WLAN device **[Col. 14, lines 12-15]**.

Regarding claim 34, Ocepek teaches a computer program product for detecting a device on a network **[Fig. 7, 102]**, the computer program product comprising: code that receives from the network a packet with an address **[Fig. 6, Source field is an address field which is received by security device as stated in Col. 7, lines 39-40]**; code that compares the address with one or more registered addresses **[Col. 8, lines 54-59]**; code that determines an operating system associated with the address, when said comparing the address results in a match between the address and at least one of the registered addresses **[Col. 8, lines 59-63, source MAC address can be used to determine operating system Col. 7, lines 43-44]**; code that compares the determined operating system with one or more stored operating systems, such that at least one of the stored operating systems corresponds to the device **[Col. 8, lines 63-65, MAC address is used to determine and compare operating system as discussed in Col. 7, lines 43-44, each MAC address can tell the operating system since specific manufactures are assigned particular series of MAC addresses as applicant discussed in his application]**; and code that

indicates that the received packet corresponds to the device when the determined operating system matches at least one of the stored operating systems **[Col. 7, lines 43-55]**; and at least one data processor that executes the code **[Fig. 7, 134, Col. 8, lines 9-11]**.

However, Ocepek in Col. 7, lines 43-55 does not teach that the device is a wireless access device rather teaches the device is a server and does not teach determining a wireless device based on the first three octets of the address.

Ocepek teaches the device can be wireless access device **[Fig. 1, 20, since WAP has a MAC address the same concept can be used to identify a wireless device]** and Gray teaches determining a wireless device based on the first three octets of the address **[Col. 14, lines 12-25]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have a check for the wireless access device so that intruder can be prevented from gaining access to internal server and servers can be protected **[Col. 2, lines 16-20]** and to match the first three octets to determine if the device is a wireless device since first three octets can identify WLAN manufacturer of the device which enables to determine if the device is a WLAN device **[Col. 14, lines 12-15]**.

Regarding claim 49, Ocepek teaches a system comprising: a network **[Fig. 7, 12]**; and a processor connected to the network, wherein the processor receives one or more packets, with an address, from the network, the processor **[Fig. 7, 134]** further comprising: means for determining an operating system associated with at least one of the packets **[Col. 8, 59-63, source MAC address is used to determine operating system, Col. 7, lines 43-44]** when an Organizationally Unique Identifier included in the at least one packet represents a device **[Col. 8, lines 63-65, MAC address' first portion has organizationally unique identifier]**; means for comparing the

determined operating system with one or more device operating systems **[Col. 8, lines 63-65, MAC address is used to determine and compare operating system as discussed in Col. 7, lines 43-44, each MAC address can tell the operating system since specific manufactures are assigned particular series of MAC addresses as applicant discussed in his application]**; and means for indicating that the at least one packet corresponds to the device, when the determined operating system matches at least one of the device operating systems **[Col. 7, lines 43-55]**.

However, Ocepek in Col. 7, lines 43-55 does not teach that the device is a wireless access device rather teaches the device is a server and does not teach determining a wireless device based on the first three octets of the address.

Ocepek teaches the device can be wireless access device **[Fig. 1, 20, since WAP has a MAC address the same concept can be used to identify a wireless device]** and Gray teaches determining a wireless device based on the first three octets of the address **[Col. 14, lines 12-25]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have a check for the wireless access device so that intruder can be prevented from gaining access to internal server and servers can be protected **[Col. 2, lines 16-20]** and to match the first three octets to determine if the device is a wireless device since first three octets can identify WLAN manufacturer of the device which enables to determine if the device is a WLAN device **[Col. 14, lines 12-15]**.

Regarding claim 50, Ocepek teaches a system comprising: a network **[Fig. 1, 12]**; a first processor interfaced to the network **[Fig. 1, 24, Col. 4, lines 57-60, client device has a processor since it performs the task described in above mentioned lines]**; and a second

processor interfaced to the network, wherein the second processor receives one or more packets, with an address, from the network and the first processor **[Fig. 7, 134, Fig. 7 is a diagram of security device 10]**, the second processor further comprising means for indicating that the first processor corresponds to a device based on an address of the first processor and on an operating system of the first processor **[Col. 7, lines 43-47, source MAC address specifies the operating system]**.

However, Ocepek in Col. 7, lines 43-47 does not teach that the device is a wireless access device rather teaches the device is a server and does not teach determining a wireless device based on the first three octets of the address.

Ocepek teaches the device can be wireless access device **[Fig. 1, 20, since WAP has a MAC address the same concept can be used to identify a wireless device]** and Gray teaches determining a wireless device based on the first three octets of the address **[Col. 14, lines 12-25]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have a check for the wireless access device so that intruder can be prevented from gaining access to internal server and servers can be protected **[Col. 2, lines 16-20]** and to match the first three octets to determine if the device is a wireless device since first three octets can identify WLAN manufacturer of the device which enables to determine if the device is a WLAN device **[Col. 14, lines 12-15]**.

Regarding claim 51, Ocepek teaches a system for detecting a device on a network **[Col. 5, lines 14-15]**, said system comprising: at least one memory **[Fig. 7, 102]** comprising: code that receives from the network a packet with an address **[Fig. 6, Source field is an address field which is received by security device as stated in Col. 7, lines 39-40]**; and code that indicates

that the received packet corresponds to the device based on the address and on an operating system associated with the received packet **[Col. 7, lines 43-47, source MAC address specifies the operating system]**; and at least one processor for executing the code **[Fig. 7, 134]**.

However, Ocepek in Col. 7, lines 43-47 does not teach that the device is a wireless access device rather teaches the device is a server and does not teach determining a wireless device based on the first three octets of the address.

Ocepek teaches the device can be wireless access device **[Fig. 1, 20, since WAP has a MAC address the same concept can be used to identify a wireless device]** and Gray teaches determining a wireless device based on the first three octets of the address **[Col. 14, lines 12-25]**

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have a check for the wireless access device so that intruder can be prevented from gaining access to internal server and servers can be protected **[Col. 2, lines 16-20]** and to match the first three octets to determine if the device is a wireless device since first three octets can identify WLAN manufacturer of the device which enables to determine if the device is a WLAN device **[Col. 14, lines 12-15]**.

Regarding claim 52, Ocepek teaches a computer program product, tangibly embodied in a computer-retable storage medium, for detecting a device on a network and containing instructions which, when executed on a processor, perform a method **[Fig. 7, 102]** comprising: receiving from the network a packet with an address **[Fig. 6, Source field is an address field which is received by security device as stated in Col. 7, lines 39-40]**; and indicating that the received packet corresponds to the device based on the address and on an operating system

associated with the received packet **[Col. 7, lines 43-47, source MAC address specifies the operating system]**.

However, Ocepek in Col. 7, lines 43-47 does not teach that the device is a wireless access device rather teaches the device is a server and does not teach determining a wireless device based on the first three octets of the address.

Ocepek teaches the device can be wireless access device **[Fig. 1, 20, since WAP has a MAC address the same concept can be used to identify a wireless device]** and Gray teaches determining a wireless device based on the first three octets of the address **[Col. 14, lines 12-25]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have a check for the wireless access device so that intruder can be prevented from gaining access to internal server and servers can be protected **[Col. 2, lines 16-20]** and to match the first three octets to determine if the device is a wireless device since first three octets can identify WLAN manufacturer of the device which enables to determine if the device is a WLAN device **[Col. 14, lines 12-15]**.

7. Claims 6, 23, 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ocepek et al. (USPN 7,124,197) in view of Gray et al. (USPN 7,295,524) and Moran (USPN 6,009,423).

Regarding claims 6, 23, 38, the references teach a method, a system and a computer program product as discussed in rejection of claim 2, 19, 34 respectively.

However, the references do not teach comparing the address further comprises: determining whether a portion of the address is similar to a portion of at least one of the registered addresses.

Moran teaches comparing based on determination of whether a portion of the address is similar to a portion of at least one of the registered addresses **[Col. 4, lines 27-34]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to match only a portion of the address so that only small search tables would have to be searched **[Col. 4, lines 56-67 – Col. 5, lines 1-2]**.

8. Claims 8, 25, 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ocepek et al. (USPN 7,124,197) in view of Gray et al. (USPN 7,295,524) and Lausier (USPN 7,174,373).

Regarding claims 8, 25, 40, the references teach a method, a system and a computer program product as discussed in rejection of claim 2, 19, 34 respectively.

However, the references do not teach determining the operating system at the IP address associated with the address.

Lausier teaches determining the operating system at the IP address associated with the address **[Col. 29, lines 20-25]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to determine the operating system associated with the IP address so that components of IP address can be assigned to a specific server **[Col. 29, lines 43-48]**.

9. Claims 9, 26, 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ocepek et al. (USPN 7,124,197) in view of Gray et al. (USPN 7,295,524) and Lausier (USPN 7,174,373) as applied to claim 8 above, and further in view of Tarquini et al. (USPG-PUB 2003/0101353).

Regarding claims 9, 26, 41, the references a method, a system and a computer program product as discussed in rejection of claims 8, 25, 34 respectively.

However, the references do not teach determining the operating system using an nmap.

Tarquini teaches determining the operating system using an nmap **[Page 7-8, Paragraph 45]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to determine the operating system using nmap so that it could be determined what operating system is a device running **[Page 3, Paragraph 13]**.

10. Claims 15, 16, 32, 33, 47, 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ocepek et al. (USPN 7,124,197) in view of Gray et al. (USPN 7,295,524) and Jennings et al. (USPN 6,580,712).

Regarding claims 15, 32, 47, the references teach a method, a system and a computer program product as discussed in rejection of claims 14, 31, and 46 respectively.

However, the references do not teach storing the plurality of the organizationally unique identifiers, such that a more frequently encountered organizationally unique identifier is searched before a less frequently encountered organizationally unique identifier.

Jennings teaches storing the plurality of the organizationally unique identifiers, such that a more frequently encountered organizationally unique identifier is searched before a less frequently encountered organizationally unique identifier **[Col. 5, lines 50-52, first portion of MAC address has Organizationally unique identifier]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to store such that more frequently used identifiers are searched first to improve the performance of searching **[Col. 5, lines 47-48]**.

Regarding claims 16, 33, 48, the references teach a method, a system and a computer program product as discussed in rejection of claims 14, 19, 48 respectively.

However, the references do not teach storing the stored operating system, such that a more frequently encountered stored operating system is searched before a less frequently encountered stored operating system.

Jennings teaches storing the stored operating system, such that a more frequently encountered stored operating system is searched before a less frequently encountered stored operating system **[Col. 5, lines 50-52, MAC address can be used to determine operating system which is well-know in the art and applicant discusses this in his specification also and by storing the MAC addresses that are accessed most, the stored operating system will be stored in a such a way also]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to store such that more frequently used identifiers are searched first to improve the performance of searching **[Col. 5, lines 47-48]**.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chandrahas Patel whose telephone number is (571)270-1211. The examiner can normally be reached on Monday through Thursday 7:30 to 17:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ricky Ngo can be reached on 571-272-3139. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ricky Ngo/
Supervisory Patent Examiner, Art Unit 2616

/Chandrahas Patel/
Examiner, Art Unit 2616